Lenovo

Lenovo XClarity Management Hub
安装和用户指南

版本 2.1

注

使用此信息及其支持的产品之前，请阅读一般声明和法律声明（位于 **XClarity Orchestrator** 在线文档）。

第二版 (2024 年 7七月)

目录

第 1 章　规划 Lenovo XClarity Management Hub

为了帮助您规划 **Lenovo XClarity Management Hub** 的安装，请仔细查看以下注意事项和先决条件。

受支持的硬件和软件

确保您的环境满足 **Lenovo XClarity Management Hub** 的硬件和软件要求。

主机系统

虚拟机监控程序要求

支持使用以下虚拟机监控程序安装 **Lenovo XClarity Management Hub**。

- **VMware ESXi 7.0**、**U1**、**U2** 和 **U3**
- **VMware ESXi 6.7**、**U1**、**U2**[1] 和 **U3**

对于 **VMware ESXi**，虚拟设备为 **OVF** 模板。

重要：

- 对于 **VMware ESXi 6.7 U2**，必须使用 **ISO** 映像 **VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso** 或更高版本。

硬件要求

下表列出了基于受管边缘客户端设备数量的 **XClarity Management Hub** *建议最低配置*。根据具体环境，可能需要其他资源才能达到最佳性能。

受管边缘客户端设备的数量	处理器	内存	存储
0 - 100 个设备	**6**	**32 GB**	**340 GB**
100 - 200 个设备	**8**	**34 GB**	**340 GB**
200 - 400 个设备	**10**	**36 GB**	**340 GB**
400 - 600 个设备	**12**	**40 GB**	**340 GB**
600 - 800 个设备	**14**	**44 GB**	**340 GB**
800 - 1000 个设备	**16**	**48 GB**	**340 GB**

1. 这是 **XClarity Management Hub** 虚拟设备用作固态硬盘数据存储的最小存储量。

软件要求

XClarity Management Hub需要下列软件。

- **NTP 服务器**。需要网络时间协议（NTP）服务器以确保从资源管理器和受管设备收到的所有事件和警报的时间戳与 **XClarity Management Hub** 同步。确保可通过管理网络（通常为 **Eth0** 接口）访问 **NTP** 服务器。

可管理的设备

XClarity Management Hub 最多可管理、监控和配置 **10,000** 个 **ThinkEdge** 客户端设备（无主板管理控制器）。

您可以从 **XClarity Management Hub** 服务器中找到受支持的 **ThinkEdge** 客户端设备和选件（例如 **I/O**、**DIMM** 和存储适配器）、所需的最低固件级别以及限制注意事项的完整列表。

有关特定设备的硬件配置和选件的常规信息，请参阅 **Lenovo Server Proven** 网页。

Web 浏览器

XClarity Management Hub Web 界面可与以下 **Web** 浏览器搭配使用。

- **Chrome 80.0** 或更高版本
- **Firefox ESR 68.6.0** 或更高版本
- **Microsoft Edge 40.0** 或更高版本
- **Safari 13.0.4** 或更高版本（在 **macOS 10.13** 或更高版本上运行）

防火墙和代理服务器

某些服务和支持功能（包括 **Call Home** 和保修状态）需要访问 **Internet**。如果网络中有防火墙，请配置防火墙以允许 **XClarity Orchestrator** 和资源管理器执行这些操作。如果 **Lenovo XClarity Orchestrator** 和资源管理器没有 **Internet** 直接访问权限，请配置它们以使用代理服务器。

防火墙

确保在防火墙上为 **XClarity Orchestrator** 和适用的资源管理器（**Lenovo XClarity Management Hub 2.0**、**Lenovo XClarity Management Hub** 和 **Lenovo XClarity Administrator**）开放以下 **DNS** 名称和端口。每个 **DNS** 代表一个具有动态 **IP** 地址且地理位置分散的系统。

注：IP 地址可能发生变化。请尽可能使用 **DNS** 名称。

DNS 名称	端口	协议
下载更新（管理软件更新、固件更新、**UpdateXpress System Pack**（操作系统设备驱动程序）和存储库包）		
download.lenovo.com	443	https
support.lenovo.com	443 和 80	https 和 http
将服务数据发送到 Lenovo 支持中心（Call Home）– 仅限 XClarity Orchestrator		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com（XClarity Orchestrator v2.0 及更高版本） rsgw-eservice.motorola.com（XClarity Orchestrator v1.6） supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx（XClarity Orchestrator v1.5 及更低版本）	443	https
向 Lenovo 发送定期数据 – 仅限 XClarity Orchestrator		

DNS 名称	端口	协议
esupportwebapi.lenovo.com（XClarity Orchestrator v2.0 及更高版本） rsgw-eservice.motorola.com（XClarity Orchestrator v1.6） supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/upload-Snapshot.ashx（XClarity Orchestrator v1.5 及更低版本）	443	https
检索保修信息		
supportapi.lenovo.com	443	https 和 http

代理服务器

如果 XClarity Orchestrator 或资源管理器没有 Internet 直接访问权限，请确保将其配置为使用 HTTP 代理服务器（请参阅XClarity Orchestrator 在线文档中的配置网络）。

- 确保代理服务器设置为使用基本认证。
- 务必将代理服务器设置为非终止代理。
- 务必将代理服务器设置为转发代理。
- 确保负载均衡器配置为保持与一个代理服务器之间的会话而不在二者之间切换。

注意： XClarity Management Hub 必须能够直接访问 Internet。当前不支持 HTTP 代理服务器。

端口可用性

Lenovo XClarity Orchestrator 和资源管理器要求某些端口处于开放状态以方便通信。如果所需的端口被阻止或由另一进程使用，则某些功能可能无法正常执行。

XClarity Orchestrator、Lenovo XClarity Management Hub 2.0、Lenovo XClarity Management Hub 和 Lenovo XClarity Administrator 是 RESTful 应用程序，使用端口 443 通过 TCP 进行安全通信。

XClarity Orchestrator

XClarity Orchestrator 通过下表中列出的端口进行侦听和响应。如果 XClarity Orchestrator 和所有受管资源受防火墙保护，而您要从防火墙*以外*的浏览器访问这些资源，请确保所需的端口处于开放状态。

注： 可以选择将 XClarity Orchestrator 配置为建立与外部服务（如 LDAP、SMTP 或 syslog）的出站连接。这些连接可能需要未包含在该列表中的其他常规用户可配置端口。这些连接也可能需要在 TCP 或 UDP 端口 53 上访问域名服务（DNS）服务器以解析外部服务器名称。

服务	出站（端口在外部系统上打开）	入站（端口在 XClarity Orchestrator 设备上开放）
XClarity Orchestrator 设备	• DNS – 端口 53 上的 TCP/UDP	• HTTPS – 端口 443 上的 TCP
外部认证服务器	• LDAP– 端口 389[1] 上的 TCP	不适用

服务	出站（端口在外部系统上打开）	入站（端口在 XClarity Orchestrator 设备上开放）
事件转发服务	• 电子邮件服务器（SMTP） – 端口 25[1] 上的 UDP • REST Web 服务（HTTP） – 端口 80[1] 上的 UPD • Splunk – 端口 8088[11] 和 8089[1] 上的 UDP • Syslog – 端口 514[1] 上的 UDP	不适用
Lenovo 服务（包含 Call Home）	• HTTPS（Call Home） – 端口 443 上的 TCP	不适用

1. 这是默认端口。可从 XClarity Orchestrator 的用户界面中配置此端口。

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 需要开放某些端口以便通信。如果所需的端口被阻止或由另一进程使用，则某些 Management Hub 功能可能无法正常执行。

如果设备位于防火墙后方，并且如果要从该防火墙外部的 Management Hub 管理这些设备，则必须确保 Management Hub 与每个受管设备上的主板管理控制器之间进行通信所涉及的所有端口均开放。

服务或组件	出站（端口对外部系统开放）	入站（端口在目标设备上开放）
XClarity Management Hub 2.0	• DNS - 端口 53 上的 UDP • NTP - 端口 123 上的 UDP • HTTPS - 端口 443 上的 TCP • SSDP - 端口 1900 上的 UDP • DHCP - 端口 67 上的 UDP	• HTTPS - 端口 443 上的 TCP • SSDP Reploy - 端口 32768-65535 上的 UDP
ThinkSystem 和 ThinkAgile 服务器	• HTTPS – 端口 443 上的 TCP • SSDP 发现 – 端口 1900 上的 UDP	• HTTPS – 端口 443 上的 TCP

XClarity Management Hub

XClarity Management Hub 通过下表中列出的端口进行侦听和响应。

服务或组件	出站（端口在外部系统上打开）	入站（端口在 XClarity Management Hub 设备上打开）
XClarity Management Hub 设备[1]	• DNS – 端口 53[2] 上的 TCP/UDP	• HTTPS – 端口 443 上的 TCP • MQTT – 端口 8883 上的 TCP
ThinkEdge 客户端设备[3]	不适用	• MQTT – 端口 8883 上的 TCP

1. 使用 XClarity Management Hub 通过 XClarity Orchestrator 管理设备时，必须开放某些端口以便通信。如果所需的端口被阻止或由另一进程使用，则某些 XClarity Orchestrator 功能可能无法正常执行。
2. 可以选择将 XClarity Management Hub 配置为建立与外部服务的出站连接。这些连接也可能需要在 TCP 或 UDP 端口 53 上访问域名服务（DNS）服务器以解析外部服务器名称。

3. 如果可管理的设备位于防火墙后方，并且如果要从该防火墙外部的 **XClarity Management Hub** 管理这些设备，则必须确保 **XClarity Management Hub** 与边缘设备之间进行通信所涉及的所有端口均开放。

XClarity Administrator

使用 **Lenovo XClarity Administrator** 通过 **Lenovo XClarity Orchestrator** 管理设备时，必须开放某些端口以便通信。如果所需的端口被阻止或由另一进程使用，则某些 **XClarity Orchestrator** 功能可能无法正常执行。

如需了解哪些端口必须为 **XClarity Administrator** 开放，请参阅端口可用性**XClarity Administrator** 在线文档中的。

网络注意事项

可配置 **Lenovo XClarity Management Hub** 来使用单个网络接口（**eth0**）或两个不同的网络接口（**eth0** 和 **eth1**）进行通信。

Lenovo XClarity Management Hub 通过以下网络进行通信。

- *管理网络* 用于 **Lenovo XClarity Management Hub** 与受管设备之间的通信。
- *数据网络* 用于在服务器上安装的操作系统与公司内部网和/或 **Internet** 之间进行通信。

单个接口（eth0）

使用单个网络接口（**eth0**）时，通过同一网络进行管理通信、数据通信和操作系统部署。

设置 **Lenovo XClarity Management Hub** 时，请遵照以下注意事项定义 **eth0** 网络接口。

- 该网络接口必须配置为支持设备发现和管理（包括固件更新）。**Lenovo XClarity Management Hub** 必须能够与其将通过管理网络管理的所有设备进行通信。**Lenovo XClarity Management Hub** 必须能够与其将通过网络管理的所有设备进行通信。
- 要部署操作系统映像，**eth0** 接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。
- **重要**：实现共享数据和管理网络可能会导致流量中断，如丢弃数据包或管理网络连接问题，具体取决于网络配置（例如，来自服务器的流量具有高优先级，而来自管理控制器的流量具有低优先级）。除 **TCP** 之外，管理网络还使用 **UDP** 流量。当网络流量较高时，**UDP** 流量可能具有较低的优先级。

两个不同的接口（eth0 和 eth1）

使用两个网络接口（**eth0** 和 **eth1**）时，可将网络设置为物理隔离或虚拟隔离的网络。

定义 **eth0** 和 **eth1** 网络接口时，请查看以下注意事项。

- **eth0** 网络接口必须连接到管理网络，并且必须配置为支持设备发现和管理。**Lenovo XClarity Management Hub** 必须能够与其将通过管理网络管理的所有设备进行通信。
- **eth1** 网络接口可配置为与内部数据网络和/或公共数据网络进行通信。
- 要部署操作系统映像，**eth1** 网络接口必须通过 **IP** 网络连接到用于访问主机操作系统的服务器网络接口。
- 可在任一网络上执行相关功能。

- 对于虚拟隔离的网络，通过同一物理连接发送来自管理网络的数据包和来自数据网络的数据包。可对所有管理网络数据包使用 **VLAN** 标记来隔离两个网络之间的流量。

IP 地址注意事项

在配置网络之前，请查看以下 **IP** 地址注意事项。

- 如果在 **XClarity Management Hub** 启动并开始运行后更改虚拟设备 **IP** 地址，将导致与 **XClarity Orchestrator** 和所有受管设备的连接发生问题。如果需要更改 **IP** 地址，请先断开 **XClarity Management Hub** 与 **XClarity Orchestrator** 的连接并终止管理所有受管设备，然后在 **IP** 地址更改完成后重新管理相应设备并将 **XClarity Management Hub** 重新连接到 **XClarity Orchestrator**。
- 配置设备和组件时尽量少更改 **IP** 地址。考虑使用静态 **IP** 地址代替动态主机配置协议（**DHCP**）。如果使用 **DHCP**，请确保尽可能减少 **IP** 地址变化，例如使 **DHCP** 地址基于 **MAC** 地址或配置 **DHCP** 以使租约不会过期。如果受管设备（**ThinkEdge** 客户端设备除外）的 **IP** 地址发生更改，必须终止管理该设备，然后再次对其进行管理。
- 不支持网络地址转换（**NAT**，用于将一个 **IP** 地址空间映射到另一个中）。
- 必须为网络接口配置 **IPv4** 地址才能管理以下设备。不支持 **IPv6** 地址。
  - **ThinkServer** 服务器
  - **Lenovo Storage** 设备
- 不支持使用 **IPv6** 链路本地地址通过数据端口或管理端口来管理 **RackSwitch** 设备。

高可用性注意事项

要为 **Lenovo XClarity Orchestrator** 设置高可用性，请使用作为主机操作系统一部分的高可用性功能。

Microsoft Hyper-V

可使用为 **Hyper-V** 环境提供的高可用性功能。

VMware ESXi

在 **VMware High Availability** 环境中，将多个主机配置为一个集群。共享存储用于制作对集群中主机可用的虚拟机（虚拟机）的磁盘映像。一次仅在一个主机上运行虚拟机。当虚拟机有问题时，将在备用主机上启动该虚拟机的另一实例。

VMware High Availability 需要以下组件。

- 最少两个装有 **ESXi** 的主机。这些主机将成为 **VMware** 集群的一部分。
- 第三个装有 **VMware vCenter** 的主机。

  提示：确保所安装的 **VMware vCenter** 版本与要在集群中使用的主机上安装的 **ESXi** 版本兼容。

  可在集群中使用的某个主机上安装 **VMware vCenter**。但是，如果该主机已关闭电源或不可用，则也将无法访问 **VMware vCenter** 界面。
- 集群中所有主机均可访问的共享存储（数据存储）。可使用 **VMware** 支持的任何类型的共享存储。**VMware** 使用数据存储决定虚拟机是否应故障转移到其他主机（检测信号）。

第 2 章　配置适用于边缘客户端设备的 XClarity Management Hub

首次访问 **Lenovo XClarity Management Hub** 时，必须完成几个步骤才能初始设置 **XClarity Management Hub**。

过程

完成以下步骤以初始设置 **XClarity Management Hub**。

步骤 **1.** 登录到 **XClarity Management Hub Web** 界面。

步骤 **2.** 阅读并接受许可协议。

步骤 **3.** 创建其他用户帐户。

步骤 **4.** 配置网络访问权限，包括数据网络和管理网络的 **IP** 地址。

步骤 **5.** 配置日期和时间。

步骤 **6.** 将 **XClarity Management Hub** 注册到 **Orchestrator** 服务器。

登录到适用于边缘客户端设备的 XClarity Management Hub

可从任何与 **XClarity Management Hub** 虚拟机具有网络连接的计算机中启动 **XClarity Management Hub Web** 界面。

开始之前

务必使用以下某种支持的 **Web** 浏览器。

- **Chrome 80.0** 或更高版本
- **Firefox ESR 68.6.0** 或更高版本
- **Microsoft Edge 40.0** 或更高版本
- **Safari 13.0.4** 或更高版本（在 **macOS 10.13** 或更高版本上运行）

通过安全连接访问 **Web** 界面。务必使用 **https**。

如果远程配置 **XClarity Management Hub**，则必须与同一第 **2** 层网络建立连接。在完成初始设置之前，必须从非路由地址访问该网络。因此，请考虑从另一可连接到 **XClarity Management Hub** 的虚拟机访问 **XClarity Management Hub**。例如，可从装有 **XClarity Management Hub** 的主机上的另一虚拟机访问 **XClarity Management Hub**。

XClarity Management Hub 会在 **60** 分钟后自动注销用户会话，无论活动状态如何。

过程

完成以下步骤以登录到 **XClarity Management Hub Web** 界面。

步骤 **1.** 用浏览器访问 **XClarity Management Hub** 的 **IP** 地址。

```
https://<IPv4_address>
```

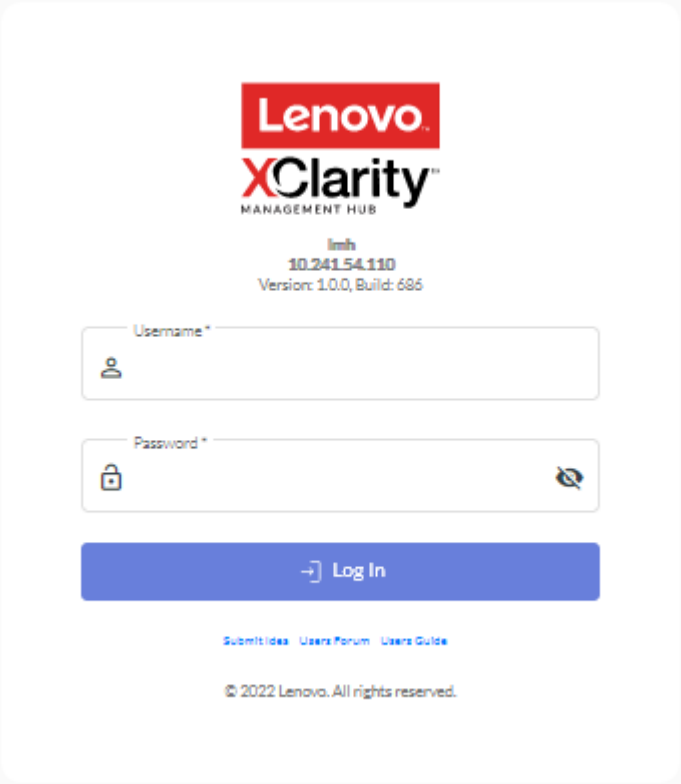
例如：

```
https://192.0.2.10
```

要使用的 **IP** 地址取决于环境设置。

- 如果在 **eth0_config** 中指定了 **IPv4** 地址，请使用该 **IPv4** 地址访问 **XClarity Management Hub**。
- 如果在与 **XClarity Management Hub** 相同的广播域中设置了 **DHCP** 服务器，请使用在 **XClarity Management Hub** 虚拟机控制台中显示的 **IPv4** 地址访问 **XClarity Management Hub**。
- 如果 **eth0** 和 **eth1** 网络在不同的子网上，并且这两个子网上均使用 **DHCP**，则在访问 **Web** 界面进行初始设置时，请使用 ***eth1*** **IP** 地址。首次启动 **XClarity Management Hub** 时，**eth0** 和 **eth1** 均获取由 **DHCP** 分配的 **IP** 地址，并将 **XClarity Management Hub** 默认网关设置为 ***eth1*** 由 **DHCP** 分配的网关。

随后将显示 **XClarity Management Hub** 初始登录页面：



步骤 **2.** 从**语言**下拉列表中选择所需的语言。

注：受管设备提供的配置设置和值可能只有英文版。

步骤 **3.** 输入您的用户凭证，然后单击**登录**。

如果是第一次登录 **XClarity Management Hub**，请输入默认凭证 **USERID** 和 **PASSW0RD**（其中 **0** 代表零）。

步骤 **4.** 阅读并接受许可协议。

步骤 **5.** 如果是第一次使用默认凭证登录，系统会提示您更改密码。默认情况下，密码必须包含 **8 – 256** 个字符，并且必须满足以下条件。

重要：建议使用 **16** 个或更多字符的高强度密码。
- (**1**) 必须包含至少一个大写字母字符
- (**2**) 必须包含至少一个小写字母字符

- (3) 必须包含至少一个数字
- (4) 必须包含至少一个特殊字符
- (5) 不能与用户名相同

步骤 6. 如果是第一次登录，系统会提示您选择是使用当前的自签名证书还是使用外部 CA 签署的证书。如果选择使用外部签署的证书，系统会显示“服务器证书”页面。

注意：自签名证书不安全。建议您生成并安装自己的外部签署证书。

有关使用外部签署证书的信息，请参阅为适用于边缘客户端设备的 XClarity Management Hub 安装可信的外部签署服务器证书。

完成之后

可从 XClarity Management Hub Web 界面右上角的**用户帐户**菜单（）中执行以下操作。

- 通过单击**注销**注销当前会话。随后将显示 XClarity Management Hub 登录页面。
- 在 Lenovo XClarity 社区论坛网站上提问和查找答案。
- 通过单击 Web 界面右上角的**用户帐户**菜单（）中的**提交意见**，或直接转到 Lenovo XClarity Ideation 网站，提交关于 XClarity Management Hub 的意见。
- 单击**用户指南**查看在线文档。
- 通过单击**关于**查看有关 XClarity Management Hub 版本的信息。
- 通过单击**更改语言**更改用户界面的语言。支持下列语言。
  - 英语（en）
  - 简体中文（zh-CN）
  - 繁体中文（zh-TW）
  - 法语（fr）
  - 德语（de）
  - 意大利语（it）
  - 日语（ja）
  - 韩语（ko）
  - 巴西葡萄牙语（pt-BR）
  - 俄语（ru）
  - 西班牙语（es）
  - 泰语（th）

为适用于边缘客户端设备的 Lenovo XClarity Management Hub 创建用户帐户

最多可为 Lenovo XClarity Management Hub 创建 10 个用户帐户。

过程

要创建用户帐户，请完成以下步骤。

步骤 1. 从 Lenovo XClarity Management Hub 菜单栏中，单击**安全性**（） → **本地用户**，以显示“本地用户”卡。

步骤 2. 单击**创建**图标（⊕）以创建用户。随后将显示创建新用户对话框。

步骤 3. 在该对话框中填写以下信息。

- 输入唯一的用户名。最多可以指定 32 个字符，包括字母数字、句点（.）、短横线（-）和下划线（_）字符。

  注：用户名不区分大小写。

- 输入新密码并确认密码。默认情况下，密码必须包含 **8 – 256** 个字符，并且必须满足以下条件。

  重要：建议使用 **16** 个或更多字符的高强度密码。
  - (**1**) 必须包含至少一个大写字母字符
  - (**2**) 必须包含至少一个小写字母字符
  - (**3**) 必须包含至少一个数字
  - (**4**) 必须包含至少一个特殊字符
  - (**5**) 不能与用户名相同

步骤 4. 单击**创建**。

该用户帐户将添加到表中。

完成之后

可从本地用户卡中执行以下操作。

- 通过单击**编辑**图标（✎）修改用户帐户的密码和属性。请注意，密码不会过期。
- 通过单击**删除**图标（🗑）删除所选用户。

为适用于边缘客户端设备的 XClarity Management Hub 配置网络设置

可以配置单个 **IPv4** 网络接口以及 **Internet** 路由设置。

开始之前

在配置网络之前查看网络注意事项（请参阅网络注意事项）。

过程

要配置网络设置，请从 **XClarity Management Hub** 菜单栏中单击**管理**（⚙）→ **网络**，然后完成以下一个或多个步骤。

- **配置 IP 设置**对于 **eth0** 接口，请单击 **Eth0 接口**选项卡，配置适用的 **IPv4** 地址设置，然后单击**应用**。

  注意：

  – 如果在 **XClarity Management Hub** 启动并开始运行后更改虚拟设备 **IP** 地址，将导致与 **XClarity Orchestrator** 和所有受管设备的连接发生问题。如果需要更改 **IP** 地址，请先断开 **XClarity Management Hub** 与 **XClarity Orchestrator** 的连接并终止管理所有受管设备，然后在 **IP** 地址更改完成后重新管理相应设备并将 **XClarity Management Hub** 重新连接到 **XClarity Orchestrator**。

  目前仅支持 **IPv4** 地址。

  – **IPv4 设置**。可配置 **IP** 分配方法、**IPv4** 地址、网络掩码和默认网关。对于 **IP** 分配方法，可选择使用静态分配的 **IP** 地址或从 **DHCP** 服务器获取 **IP** 地址。使用静态 **IP** 地址时，必须提供 **IP** 地址、网络掩码和默认网关。

    默认网关必须为有效的 **IP** 地址，并且必须与启用的接口（**eth0**）使用相同的网络掩码（同一子网）。

    如果任何一个接口使用 **DHCP** 获取 **IP** 地址，则默认网关也使用 **DHCP**。

- **配置 Internet 路由设置**（可选）从“**DNS** 配置”卡中配置域名系统（**DNS**）设置。然后，单击**应用**。

  目前仅支持 **IPv4** 地址。

  可以更改 **DNS** 服务器的 **IP** 地址。

  DNS 服务器的完全限定域名（**FQDN**）和主机名与 **XClarity Management Hub** 服务器相同，不能更改。

为适用于边缘客户端设备的 XClarity Management Hub 配置日期和时间

必须设置至少一个（最多四个）网络时间协议（NTP）服务器以同步 **XClarity Management Hub** 与所有受管设备之间的时间戳。

开始之前

必须可通过网络访问每个 **NTP** 服务器。请考虑在运行 **XClarity Management Hub** 的本地系统上设置该 **NTP** 服务器。

如果更改 **NTP** 服务器上的时间，则 **XClarity Management Hub** 可能需要一段时间才能与新时间同步。

注意：必须将 **XClarity Management Hub** 虚拟设备及其主机设置为同步到同一个时间源，以防止 **XClarity Management Hub** 及其主机之间意外失去同步。通常情况下，主机配置为使其虚拟设备与其进行时间同步。如果 **XClarity Management Hub** 设置为同步到其主机之外的其他源，则必须禁用 **XClarity Management Hub** 虚拟设备及其主机之间的主机时间同步。

- 对于 **ESXi**，请按照 **“VMware – 禁用时间同步”Web 页面**上的说明进行操作。

过程

要设置 **XClarity Management Hub** 的日期和时间，请完成以下步骤。

步骤 **1.** 从 **XClarity Management Hub** 菜单栏中，单击**管理**（⚙） **→ 日期和时间**以显示“日期和时间”卡。

步骤 2. 选择 **XClarity Management Hub** 主机所在的时区。

如果所选时区采用夏令时（**DST**），则针对 **DST** 自动调整时间。

步骤 3. 指定网络中每个 **NTP** 服务器的主机名或 **IP** 地址。最多可定义四个 **NTP** 服务器。

步骤 4. 单击**应用**。

为适用于边缘客户端设备的 Lenovo XClarity Management Hub 管理安全证书

Lenovo XClarity Management Hub 使用 **SSL** 证书在 **Lenovo XClarity Management Hub** 与其受管设备之间建立安全可信的通信以及用户或其他服务与 **Lenovo XClarity Management Hub** 的通信。默认情况下，**Lenovo XClarity Management Hub** 和 **XClarity Orchestrator** 使用 **XClarity Orchestrator** 生成的由内部证书颁发机构颁发的自签名证书。

开始之前

本节适用于对 **SSL** 标准和 **SSL** 证书的概念及管理有基本了解的管理员。有关公钥证书的常规信息，请参阅 **Wikipedia** 中的“**X.509**”网页和 “**Internet X.509** 公钥基础结构证书 和证书吊销列表（**CRL**）**Profile**（**RFC5280**）”网页。

关于本任务

在每个 **Lenovo XClarity Management Hub** 实例中唯一生成的默认服务器证书为多种环境提供充分的安全性。可让 **Lenovo XClarity Management Hub** 为您管理证书，也可更主动地定制或替换服务器证书。**Lenovo XClarity Management Hub** 可根据所处环境定制证书。例如，可决定：

- 通过重新生成内部证书颁发机构证书和/或具有组织特定值的最终服务器证书来生成一对新密钥。
- 生成证书签名请求（**CSR**），该 **CSR** 可发送到所选的证书颁发机构以签署自定义证书并上传到 **Lenovo XClarity Management Hub**，用作其所有托管服务的最终服务器证书。
- 将服务器证书下载到本地系统，以便将该证书导入到 **Web** 浏览器的可信证书列表中。

Lenovo XClarity Management Hub 提供多个接受传入 SSL/TLS 连接的服务。客户端（如 Web 浏览器）连接到其中一个服务时，Lenovo XClarity Management Hub 将提供其*服务器证书*以供尝试连接的客户端识别。客户端应保留一个其信任的证书的列表。如果 Lenovo XClarity Management Hub 服务器证书未包含在客户端的列表中，客户端将断开与 Lenovo XClarity Management Hub 的连接以避免与不可信来源进行任何安全敏感信息的交换。

在与受管设备和外部服务通信时，Lenovo XClarity Management Hub 充当客户端。在这种情况下，受管设备或外部服务会提供其服务器证书供 Lenovo XClarity Management Hub 验证。Lenovo XClarity Management Hub 会维护一个信任证书列表。如果受管设备或外部服务提供的*可信证书*未包含在该列表中，Lenovo XClarity Management Hub 将断开该受管设备或外部服务的连接以避免与不可信来源进行任何安全敏感信息的交换。

Lenovo XClarity Management Hub 服务将使用以下类别的证书，这些证书要受所连接到的任何客户端的信任。

- **服务器证书**。在初始引导期间会生成唯一密钥和自签名证书。这些证书的颁发机构将视为默认的根证书颁发机构，可在 Lenovo XClarity Management Hub 安全设置中的“证书颁发机构”页面中进行管理。除非密钥已泄露或如果您的组织有策略要求必须定期更换所有证书，否则无需重新生成此根证书（请参阅为适用于边缘客户端设备的 XClarity Management Hub 重新生成自签名服务器证书）。此外，在初始设置期间还会生成一个单独的密钥，并创建一个由内部证书颁发机构签名的服务器证书。此证书用作默认的 Lenovo XClarity Management Hub 服务器证书。每次 Lenovo XClarity Management Hub 检测到网络地址（IP 或 DNS 地址）变化时将自动重新生成该证书，以确保该证书包含服务器的正确地址。此外也可按需定制和生成该证书（请参阅为适用于边缘客户端设备的 XClarity Management Hub 重新生成自签名服务器证书）。

  可选择使用外部签署的服务器证书而不使用默认的自签名服务器证书。为此，需要生成证书签名请求（CSR），让 CSR 由私有或商业证书根证书颁发机构签名，然后将完整的证书链导入 Lenovo XClarity Management Hub 中（请参阅为适用于边缘客户端设备的 XClarity Management Hub 安装可信的外部签署服务器证书）。

  如果选择使用默认的自签名服务器证书，建议在 Web 浏览器中导入服务器证书作为可信根证书，以避免浏览器中出现证书错误消息（请参阅为适用于边缘客户端设备的 Lenovo XClarity Management Hub 将服务器证书导入到 Web 浏览器中）。
- **操作系统部署证书**。操作系统部署服务使用单独的证书来确保操作系统安装程序在部署过程中可以安全地连接到部署服务。如果密钥已泄露，可通过重新启动 Lenovo XClarity Management Hub 来重新生成密钥。

为适用于边缘客户端设备的 XClarity Management Hub 重新生成自签名服务器证书

您可以生成新的服务器证书来替换当前的自签名 Lenovo XClarity Management Hub 服务器证书，或者恢复 XClarity Management Hub 生成的证书（如果 XClarity Management Hub 当前使用定制的外部签署服务器证书）。XClarity Management Hub 将使用该新的自签名服务器证书来访问 HTTPS。

开始之前

注意：如果使用新的根 CA 重新生成 XClarity Management Hub 服务器证书，XClarity Management Hub 会失去与受管设备的连接，因此您必须重新管理这些设备。如果在不更改根 CA 的情况下重新生成 XClarity Management Hub 服务器证书（例如，当证书过期时），则无需重新管理设备。

关于本任务

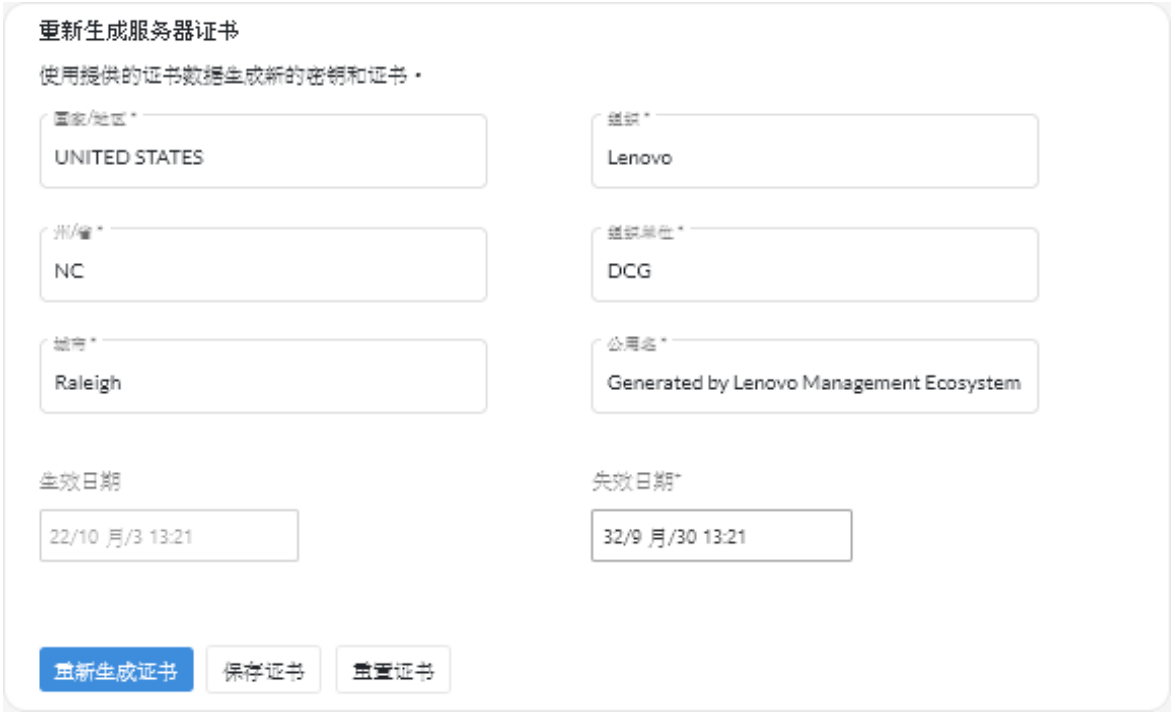
当前使用的服务器证书（无论是自签名还是外部签署）在生成、签署并安装新的服务器证书之前将继续使用。

重要：修改服务器证书后，**Management Hub** 将重新启动，所有用户会话也将结束。用户必须重新登录才能继续在该 **Web** 界面中工作。

过程

要生成自签名的 **XClarity Management Hub** 服务器证书，请完成以下步骤。

步骤 1. 从 **XClarity Management Hub** 菜单栏中，单击**安全性**（⚙）→ **服务器证书**以显示**重新生成自签名服务器证书**卡。



步骤 2. 在**重新生成自签名服务器证书**卡中，填写请求的字段。

- 用于关联证书组织的来源国家或地区的两字母 **ISO 3166** 代码（例如，美国为 **US**）。
- 与证书关联的州或省全名（例如，**California** 或 **New Brunswick**）。
- 用于关联证书的城市全名（例如，**San Jose**）。该值长度不得超过 **50** 个字符。
- 拥有证书的组织（公司）。通常为公司的合法注册名称。名称中应包含 **Ltd.**、**Inc.** 或 **Corp** 等后缀（例如，**ACME International Ltd.**）。该值长度不得超过 **60** 个字符。
- （可选）拥有证书的组织单位（例如，**ABC** 部门）。该值长度不得超过 **60** 个字符。
- 证书所有者的公用名。通常为使用证书的服务器的完全限定域名（**FQDN**）或 **IP** 地址（例如，www.domainname.com 或 192.0.2.0）。该值长度不得超过 **63** 个字符。

  注：目前，该属性对证书没有影响。
- 服务器证书失效的日期和时间。

  注：目前，这些属性对证书没有影响。

注：重新生成服务器证书时，不可更改主题备用名称。

步骤 3. 单击**重新生成自签名服务器证书**以重新生成自签名证书，然后单击**重新生成证书**进行确认。
这时 Management Hub 会重新启动，已建立的所有用户会话都会结束。

步骤 4. 重新登录到 Web 浏览器。

完成之后

您可以从“重新生成自签名服务器证书”卡中执行以下操作。

- 单击**保存证书**将当前服务器证书以 PEM 格式保存到本地系统。
- 单击**重置证书**使用默认设置重新生成服务器证书。出现提示时，按 Ctrl+F5 刷新浏览器，然后重新建立与 Web 界面的连接。

为适用于边缘客户端设备的 XClarity Management Hub 安装可信的外部签署服务器证书

您可以选择使用由私人或商业证书颁发机构（CA）签署的可信服务器证书。要使用外部签署的服务器证书，请生成证书签名请求（CSR），然后导入所得的服务器证书以替换现有服务器证书。

开始之前

注意：

- 如果使用新的根 CA 安装外部签署的 Lenovo XClarity Management Hub 服务器证书，XClarity Management Hub 会失去与受管设备的连接，因此您必须重新管理这些设备。如果在不更改根 CA 的情况下安装外部签署的 Lenovo XClarity Management Hub 服务器证书（例如，当证书过期时），则无需重新管理设备。
- 如果在生成 CSR 之后、导入已签名的服务器证书之前添加了新设备，则必须重新启动这些设备才能接收新的服务器证书。

关于本任务

最佳做法是始终使用 v3 签名证书。

必须从使用**生成 CSR 文件**按钮最新生成的证书签名请求来创建外部签署的服务器证书。

外部签署的服务器证书内容必须是包含整个 CA 签名链（其中包括 CA 的根证书、任何中间证书和服务器证书）的证书捆绑包。

如果新服务器证书未由可信的第三方签署，则下次连接到 Lenovo XClarity Management Hub 时，Web 浏览器将显示安全消息和对话框，提示您将新证书纳入浏览器。要避免显示安全消息，可将服务器证书导入到 Web 浏览器的可信证书列表中（请参阅为适用于边缘客户端设备的 Lenovo XClarity Management Hub 将服务器证书导入到 Web 浏览器中）。

XClarity Management Hub 在不终止当前会话的情况下，开始使用新的服务器证书。新会话将以新证书建立。要使用正在使用的新证书，请重新启动 Web 浏览器。

重要：修改服务器证书后，必须单击 Ctrl+F5 来刷新 Web 浏览器，然后重新建立与 XClarity Management Hub 的连接，从而让所有已建立的用户会话接受新证书。

过程

要生成并安装外部签署的服务器证书，请完成以下步骤。

步骤 1. 创建一个证书签名请求并将文件保存到本地系统。

1. 从 **XClarity Management Hub** 菜单栏中，单击**安全性**（⚙）→ **服务器证书**，以显示“生成证书签名请求”卡。

2. 在“生成证书签名请求（CSR）”卡中，填写请求的字段。
   - 与证书组织关联的来源国家或地区的两字母 **ISO 3166** 代码（例如，美国为 **US**）。
   - 与证书关联的州或省全名（例如，**California** 或 **New Brunswick**）。
   - 与证书关联的城市全名（例如，**San Jose**）。该值长度不得超过 **50** 个字符。
   - 拥有证书的组织（公司）。通常为公司的合法注册名称。名称中应包含 **Ltd.**、**Inc.** 或 **Corp** 等后缀（例如，**ACME International Ltd.**）。该值长度不得超过 **60** 个字符。
   - （可选）拥有证书的组织单位（例如，**ABC** 部门）。该值长度不得超过 **60** 个字符。
   - 证书所有者的公用名。这必须是正在使用证书的服务器的主机名。该值长度不得超过 **63** 个字符。

     注：目前，该属性对证书没有影响。
   - （可选）生成 **CSR** 时在 **X.509**“**subjectAltName**”扩展名中自定义、删除和添加的主题备用名称。仅在生成 **CSR** 后才会验证指定的主题备用名称（基于指定的类型）并将其添加到 **CSR**。默认情况下，**XClarity Management Hub** 会根据 **XClarity Management Hub** 访客操作系统的网络接口发现的 **IP** 地址和主机名自动为该 **CSR** 定义主题备用名称。

     注意：主题备用名称必须包含 **Management Hub** 的完全限定域名（**FQDN**）或 **IP** 地址，并且主题名称必须设置为 **Management Hub** 的 **FQDN**。为确保生成的证书完整，在开始 **CSR** 过程之前，请验证这些必填字段是否存在且正确。缺少证书数

据可能会导致在尝试将 Management Hub 连接到 Lenovo XClarity Orchestrator 时连接不受信任。

指定的名称必须对所选的类型有效。
- DNS（使用 FQDN，例如 hostname.labs.company.com）
- IP 地址（例如，192.0.2.0）
- 邮箱（例如，example@company.com）

步骤 2. 向可信证书颁发机构（CA）提供 CSR。CA 签署 CSR 并返回一个服务器证书。

步骤 3. 将外部签署的服务器证书和 CA 证书导入到 XClarity Management Hub，并替换当前服务器证书。

1. 从“生成证书签名请求（CSR）”卡中，单击**导入证书**以显示导入证书对话框。
2. 复制并粘贴 PEM 格式的服务器证书和 CA 证书。必须提供从服务器证书到根 CA 证书的完整证书链。
3. 单击**导入**将服务器证书存储在 XClarity Management Hub 信任存储区中。

步骤 4. 按 Ctrl+F5 刷新浏览器，然后重新建立与 Web 界面的连接，从而接受新证书。此步骤必须由所有已建立的用户会话来完成。

为适用于边缘客户端设备的 Lenovo XClarity Management Hub 将服务器证书导入到 Web 浏览器中

可将当前服务器证书的 PEM 格式副本保存到本地系统。随后可将证书导入 Web 浏览器的可信证书列表或其他应用程序中，以避免在访问 Lenovo XClarity Management Hub 时 Web 浏览器显示安全警告消息。

过程

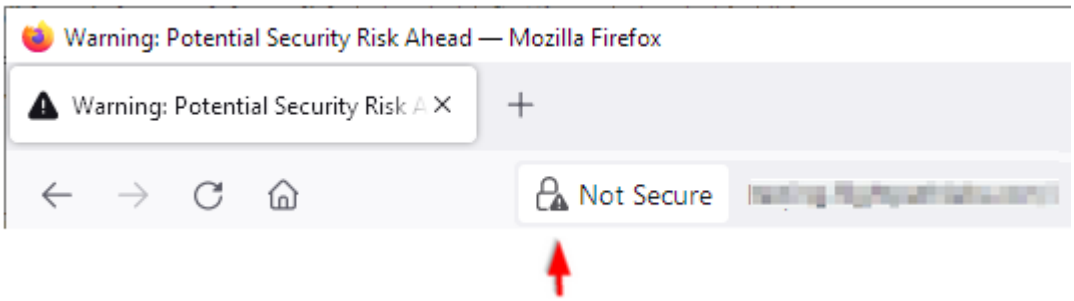
要将服务器证书导入到 Web 浏览器中，请完成以下步骤。

- Chrome
  1. 导出 Lenovo XClarity Management Hub 服务器证书。
     a. 单击顶部地址栏中的“不安全”警告图标，例如：

     b. 单击**证书无效**以显示“证书”对话框。
     c. 单击**详细信息**选项卡。
     d. 单击**导出**。
     e. 指定证书文件的名称和位置，然后单击**保存**以导出证书。
     f. 关闭“证书查看器”对话框。
  2. 将 Lenovo XClarity Management Hub 服务器证书导入到浏览器的可信根证书颁发机构证书列表中。

a. 在 Chrome 浏览器中，单击窗口右上角的三点图标，然后单击**设置**，打开“设置”页面。
b. 单击**隐私和安全**，然后单击**安全性**，以显示“安全性”页面。
c. 滚动到**高级**部分，然后单击**管理设备证书**。
d. 单击**导入**，然后单击**下一步**。
e. 选择先前导出的证书文件，然后单击**下一步**。
f. 选择证书的存储位置，然后单击**下一步**。
g. 单击**完成**。
h. 关闭并重新打开 Chrome 浏览器，然后打开 Lenovo XClarity Management Hub。

- **Firefox**
  1. 导出 Lenovo XClarity Management Hub 服务器证书。
     a. 单击顶部地址栏中的“不安全”警告图标，例如：



     b. 单击**连接不安全**，然后单击**更多信息**。
     c. 单击**查看证书**。
     d. 向下滚动到**杂项**部分，然后单击 PEM（证书）链接以将文件保存到本地系统。
  2. 将 Lenovo XClarity Management Hub 服务器证书导入到浏览器的可信根证书颁发机构证书列表中。
     a. 打开浏览器，单击**工具 → 设置**，然后单击**隐私和安全**。
     b. 向下滚动到**安全性**部分。
     c. 单击**查看证书**，以显示“证书管理器”对话框。
     d. 单击**您的证书**选项卡。
     e. 单击**导入**，然后浏览至下载该证书的位置。
     f. 选择该证书，然后单击**打开**。
     g. 关闭“证书管理器”对话框。

将适用于边缘客户端设备的 XClarity Management Hub 连接到 XClarity Orchestrator

注册（连接）Lenovo XClarity Management Hub 到 Lenovo XClarity Orchestrator 后，即可开始管理和监控设备。

开始之前

确保可从 XClarity Orchestrator 通过网络访问 XClarity Management Hub，也可从 XClarity Management Hub 通过网络访问 XClarity Orchestrator。

过程

要注册 **XClarity Management Hub**，请完成以下步骤。

步骤 **1.** 创建 **Management Hub** 注册密钥。

1. 从 **Management Hub** 菜单栏中，单击**注册**，以显示“注册”页面。

2. 单击**创建注册密钥**。
3. 单击**复制到剪贴板**复制注册密钥，然后关闭对话框。

步骤 **2.** 将 **Management Hub** 注册密钥添加到 **XClarity Orchestrator**。

1. 从 **XClarity Orchestrator** 菜单栏中，单击**资源**（⚙） → **资源管理器**以显示“资源管理器”卡。
2. 单击**连接**图标（●）显示资源管理器。“连接资源管理器”对话框。

3. 选择 **XClarity Management Hub** 作为资源管理器。
4. 将注册密钥拷贝到**注册令牌**字段中。
5. 单击**连接**以显示连接资源管理器，其中包含 **XClarity Orchestrator** 注册密钥。
6. 单击**复制到剪贴板**复制注册密钥，然后关闭对话框。

步骤 3. 将 **XClarity Orchestrator** 注册密钥添加到 **Management Hub**。

1. 从 **Management Hub** 菜单栏中，单击**注册**以显示“注册”页面。
2. 单击**安装注册密钥**。
3. 将注册密钥拷贝到**注册令牌**字段中。
4. 单击**连接**。

完成之后

- 使用 **Management Hub** 管理设备（请参阅**XClarity Orchestrator** 在线文档中的管理 **ThinkEdge** 客户端设备）。
- 通过单击**重置注册**删除当前的 **Management Hub** 注册密钥。

第 3 章　卸载适用于边缘客户端设备的 XClarity Management Hub

完成以下步骤以卸载 **XClarity Management Hub** 虚拟设备。

过程

要卸载 **XClarity Management Hub** 虚拟设备，请完成以下步骤。

步骤 **1.** 终止管理当前受 **XClarity Management Hub** 管理的所有设备。

步骤 **2.** 根据操作系统卸载 **XClarity Management Hub**。

- **ESXi**
  1. 通过 **VMware vSphere Client** 连接到主机。
  2. 右键单击虚拟机，然后单击**电源 → 关机**。
  3. 再次右键单击虚拟机，然后单击**从磁盘中删除**。